MM2211 Wireless Broadband Gateway

MM2211 Wireless Broadband Gateway User's Guide

Part number: 8000013

July 2006

Trademarks

Ruckus Wireless, BeamFlex™, MediaFlex™, MediaFlex 2900 Multimedia Access Point, MF2900 AP, and MM2211 Wireless Broadband Gateway are trademarks of Ruckus Wireless Web Interface

All other brand and product names are registered trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Ruckus Wireless, Inc. reserves the right to make changes to the products described in this document without notice.

Ruckus Wireless, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

The device has met the FCC 15.247 requirement. In order to comply with the FCC RF exposure requirement, the user must keep 20cm away from the antenna.

This device has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this device does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

• Reorient or relocate the receiving antenna.

• Increase the separation between the equipment and receiver.

• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

• Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Information to the user

The user's manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

EN 55 022 Declaration of Conformance

This is to certify that the MM2211 MetroFlex Wireless Access Gateway is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

Contents

Preface

This   MM2211 Wireless Broadband Gateway User's Guide will help you understand the MM2211 Wireless Broadband Gateway, how to install it, and configure it using the Ruckus Wireless Web Interface.

Who Should Use this Guide

This User's Guide assumes that the reader has basic to intermediate computer and Internet skills. All the basic computer networking, Internet, and other information required to configure this device is provided herein.

What You'll Find in this Guide

The following topics are covered:

- Chapter 1: "Introduction"
- Chapter 2: "Installation and Setup"
- Chapter 3: "Using the Ruckus Wireless Web Interface"
- Appendix A: "Technical Specifications"

Typographic conventions

This User's Guide uses the following typographic conventions:

Table 1—Typographic conventions

Typeface or Symbol	Meaning	Example
italics	Emphasis, book titles, CD names, special terms. Also used to denote optional input if surrounded by *<brackets>*	Read your *User's Guide* thoroughly. Enter an address in the range `192.168.0.<2-253>`
bold	System menu names, user input	Open the **Control Panel**.
fixed	Screen text, URLs, IP addresses	Browse to the following IP address: http://192.168.0.254

System Requirements

The MM2211 Wireless Broadband Gateway is compatible with most contemporary personal computers and operating systems that are configured for Internet and wireless networking.

The MM2211 Wireless Broadband Gateway is accessed and configured via a Web browser interface. Any of the following Web browsers are supported:

- Microsoft Internet Explorer 5.0 and higher
- Netscape version 6.0 and higher
- Apple Safari 1.0 and higher
- Mozilla Firefox version 1.0 and higher

Support and Warranty Information

See the *Warranty and Support* card for detailed information about contacting Technical Support, and the Warranty terms for your MM2211 Wireless Broadband Gateway.

Chapter 1: Introduction

Congratulations on your purchase of the MM2211 Wireless Broadband Gateway. The MM2211 is a purpose-built home gateway designed to deliver the best possible connectivity from subscriber homes to Mesh Networks. Mesh Networks provide coverage across wide areas using a mesh distribution of access points based on standard Wi-Fi protocols.

The installation uses outdoor high power Mesh routers to achieve coverage for outdoor wireless devices. Typically, the indoor coverage is inadequate to maintain an acceptable quality level for users within the home. The MM2211 is a Customer Premise Equipment to allow the extension of the Metro Wi-Fi signals to achieve a robust coverage within home. The MM2211 communicates with the Mesh Networks routers to allow home devices (such as PC or laptops) to access the Internet.

A typical installation consists of a Ruckus Wireless, Inc. MM2211 Wireless Broadband Gateway connected to a PC. The MM2211 Gateway receives wireless signals from outdoor Mesh Routers or other remote AP that is connected to a DSL router or cable modem. Data traffic is distributed to all devices connected behind the MM2211 Wireless Broadband Gateway.
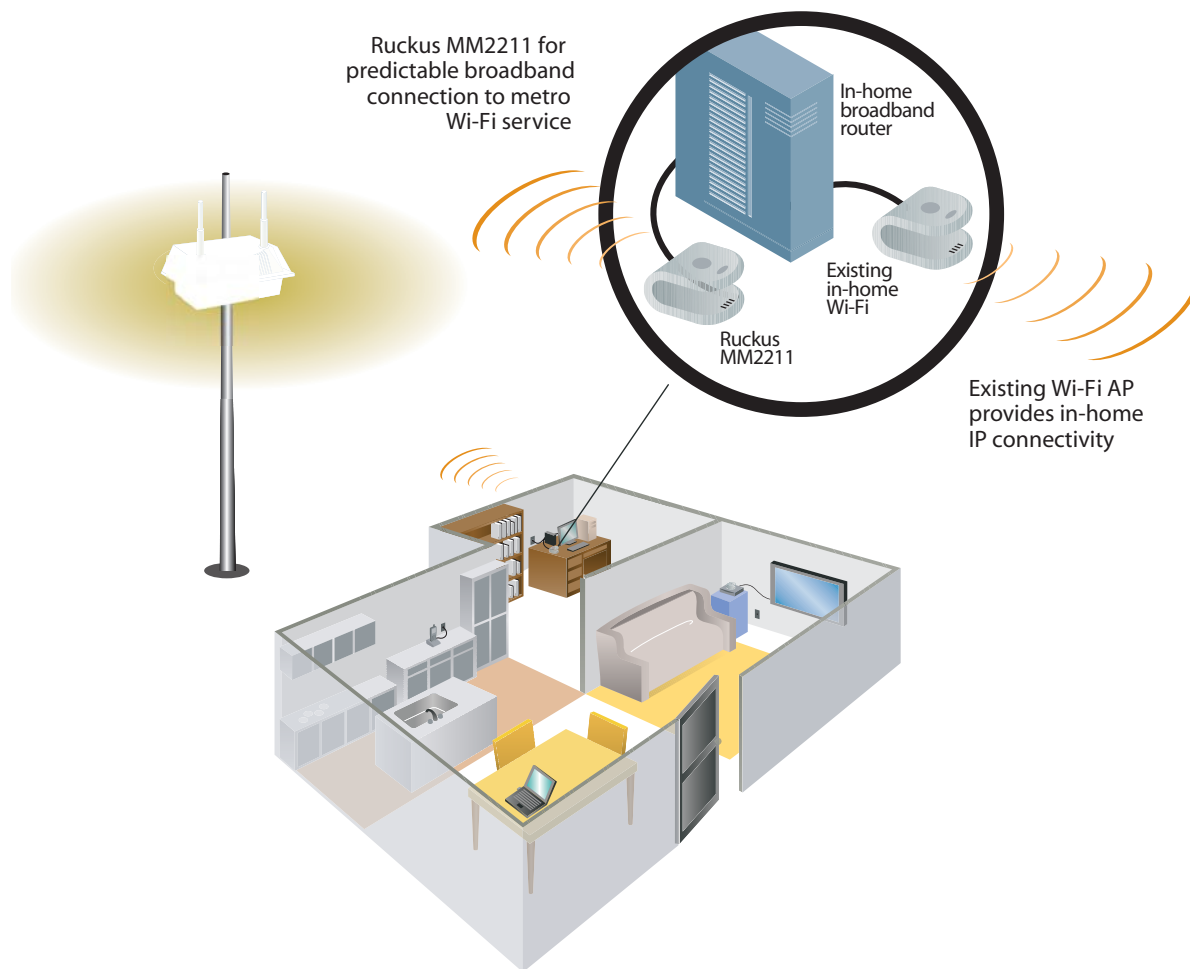

Figure 1—The MM2211 Wireless Broadband Gateway in a Typical Home Network

MetroFlex™

MetroFlex™ is Ruckus Wireless, Inc.'s family of purpose-built, multimedia Wi-Fi appliances that enable reliable wireless metro-area wi-fi network access.

BeamFlex™

BeamFlex™ is Ruckus Wireless, Inc.'s patent-pending antenna technology that allows wireless signals to navigate around interference, extend wireless signal range, and increase speeds and capacity for 802.11b/g wireless networks. The BeamFlex™ antenna system consists of an array of six high-gain antenna elements, that allow the MM2211 to find quality signal paths in a changing environment, and sustain the baseline performance required in a metro wi-fi environment.

MetroFlex enhances the existing BeamFlex technology to use a dual polarized (horizontal and vertical) antenna array.

Key Features

BeamFlex™ Smart MIMO Antenna Maximizes Wireless Range and Performance

- Multi-In, Multi-Out (MIMO) technology supports real time learning of radio frequency, station, network and application conditions.

- On-the-fly adaptation to each receiving device in response to environmental changes such as interference to maximize signal quality, data rate and minimize packet errors and retransmissions.

- Internal driver software controls an antenna array with 6 high-gain, directional antenna elements and 63 unique antenna combinations.

- Expert system 802.11 driver controls data rate and retransmission policies on a per-packet basis.

Simple Configuration and Installation

- Simple Web-based user interface for easy configuration and customization of features such as SSID, WEP or WPA key, statistics monitoring and software upgrade.

Standards-based Solution Protects User Investment, Minimizes Replacement Cost

- Compliant with 802.11b and 802.11g: supports 802.11g wireless networking at up to 54 Mbps; and can interoperate in 802.11g-only or mixed networks.

- Supports Wi-Fi Protected Access-Pre-Shared Key (WPA-PSK) data encryption. WPA provides strong data encryption and authentication based on a pre-shared key.

- Supports 64-bit and 128-bit WEP encryption security. WEP keys can be generated manually or by passphrase.

- Attaches to home PC by Ethernet to optimize the reception of wireless signals from the outdoor Mesh Networks nodes.

- Forward compatible with the emerging 802.11n WLAN standard.

Chapter 2: Installation and Setup

This chapter describes how to install your MM2211 Wireless Broadband Gateway, and how to set up your PC to connect to the Ruckus Wireless Web Interface.

Topics covered in this chapter include:

Packing List

1. MM2211 Wireless Broadband Gateway

2. AC power adapter (Input DC 5-18V 1-2A)

3. Category 5 (CAT5) Ethernet Cable

MM2211 Wireless Broadband Gateway

Front View

Figure 2— "Front View of the MM2211 Wireless Broadband Gateway" shows the front view MM2211 Gateway, with the LED indicators numbered. The numbers correspond to the labels describing LED behavior in Table 2— "LED Indicators and Meanings" on page 13.

Figure 2—*Front View of the MM2211 Wireless Broadband Gateway*

LED Status Lights

Table 2— "LED Indicators and Meanings" describes the LED lights on the front of the MM2211 Gateway.

Table 2—LED Indicators and Meanings

Label	LED	Activity	Description
1	Power	Green Off	Power is supplied to the MM2211 Gateway. Power is not supplied to the MM2211 Gateway.
2	LAN	Green Steady Off	The MM2211 Gateway has link. The MM2211 Gateway has no link.
3	Wireless	Green Flashing Green Steady	The MM2211 Gateway is transmitting data. The faster the flashing, the more data is being transmitted or received. The Wireless port is initialized and enabled.
4	Air Quality	Green Steady Green Flashing Green intermittent Flashing	**Good Air Quality:** A steady Green LED indicates that the current environment will support quality data transmission. **Marginally Acceptable Air Quality:** a flashing Green LED (on for 0.25 second, off 0.25 second) indicates that the current environment does not always meet the data transmission standard. While data transmission is possible, the quality will vary. **Bad Air Quality:** A briefly flashing Green LED (on for 0.03 second and off for 1 second) indicates that data transmission is not possible in the current environment. The brief flash also indicates that the device is still functioning.

Rear View

Figure 3—Rear View of the MM2211 Gateway

Table 3—Rear Ports and Adapters

Label	Description
6	AC Power Adapter (Input: DC 5V 1A)
7	10/100 Mbps Auto-sensing, autonegotiating RJ-45 network port
8	Reset button. Used only if you need to reset the MM2211 Gateway to its factory default settings. Insert the end of a paper clip or pin into the hole and hold it in for at least 8 seconds.
9	Push button. Not operational in current release.

Placement Guidelines

You or your service provider or installer can determine the best placement for the MM2211 Gateway by using the following guidelines.

Establishing a Good General Location

Your MM2211 Gateway should be placed:

- On a shelf or other elevated location away from any physical obstructions.

- Away from other sources of electromagnetic interference (for example, microwave ovens, and cordless
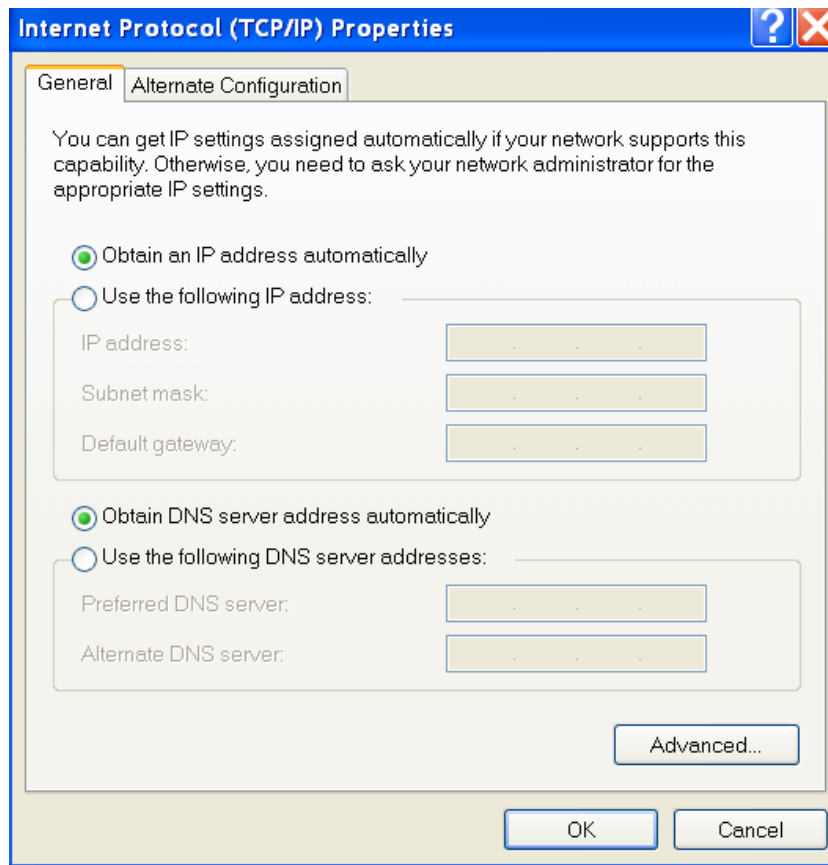
Figure 4—*Internet Protocol (TCP/IP) Properties*

5. Select **Obtain an IP address automatically**, and click OK to exit the *TCP/IP Properties* window.

6. Click **OK** to exit the Local Area Connection Properties window.

Connect and Configure Your Ruckus MM2211 Gateway

The following steps will guide you to set up and gain administrative access to your Ruckus MM2211 Metro Broadband Gateway.

1. Remove the Ruckus MM2211 Metro Broadband Gateway from the packaging and place it next to your computer.

2. Connect the AC power supply to the Ruckus MM2211 gateway and plug the other end into a power outlet or to a surge protector that is plugged into a power outlet.

3. Connect the CAT5 Ethernet cable to the Ethernet port on your computer, and to the Ethernet port on the Ruckus MM2211 Metro Broadband Gateway.

4. On your PC, open a browser window. Enter the address http://192.168.1.1.

5. When the login screen appears, enter the username **admin** and the password as **password**. Then click the Login button.

After logging in, you will see the main information page. On the information page, there are two panes. The pane on the left shows major information or configuration points. Each major information or configuration area has a number of sub-menus. Clicking on the relevant menu will bring the relevant page onto the screen.

The system monitors the activities on the Web user interface. If you do not use the Web interface for more than five minutes, the system will time out, and you will be logged out automatically. You need to re-log in to access the interface.

6. In the *Configuration->Wireless* menu, you may change the default wireless network Name (SSID) for this device to match the SSID of the AP you intend to connect to.

7. Refer to the information provided under the Help button before attempting to change any other default settings in this screen.

8. The initial configuration is now complete. Click **Reboot/Reset** to make the change take effect.

CAUTION:—Make sure to write down the new IP address, username, password and SSID. If you change the MM2211 Gateway's default IP address to one outside the current address range of your PC, you will not be able to connect to the device after reboot until you reset your computer's IP address to be within the same network as the MM2211 Gateway. See Table 4, "Wireless Network Settings Worksheet," on page 20 and Table 5, "MM2211 Gateway Default and User Settings Worksheet," on page 21 for more information.

You should now be able to find the default SSID of your MM2211 Gateway over your wireless connection:

Accessing the Web Interface

*CAUTION:—Any configuration changes will be lost unless you use the **Update** button. It is recommended that after each configuration screen you modify, you click the **Update** button.*

Chapter 3: Using the Ruckus Wireless Web Interface

This chapter describes the tasks you need to do to customize the MM2211 Gateway to run on your wireless network.

Topics covered in this chapter include:

Wireless Settings Worksheet

Before you modify any wireless settings on the MM2211 Gateway, print Table 4— "Wireless Network Settings Worksheet" and record the following information about your wireless network. Your ISP or network administrator may provide you with this information. The wireless information recorded in this worksheet should be used to configure the MM2211 Gateway's wireless settings.

Table 4—Wireless Network Settings Worksheet

Item	Description and Your Network Setting
MM2211 Gateway SSID	The SSID identifies the remote AP. Make sure to specify the SSID of the Mesh Networks Router, or the SSID as defined by the Metro ISP provider.Once you obtain the SSID from the Metro ISP provider, this is the value you must enter as the MM2211 Gateway SSID. You can use up to 32 alphanumeric characters. The SSID *is* case sensitive.
Security	If using WEP, circle the method used: [Open System] [Shared Key] [Auto} Circle the type of Shared key: 64-bit 128 bit Passphrase method • If using 64-bit WEP: use 10 hex digits (any combination of **0-9** or **a-f)** or 5 ascii characters • If using 128-bit WEP, use 26 hex digits or 13 ascii characters The WEP key values are *not* case-sensitive. **Key 1** _____ **Key 2** _____ **Key 3** _____ **Key 4** _____ If using WPA-PSK, write down the passphrase. The WPA-PSK passphrase *is* case-sensitive. **WPA Passphrase:** _____

MM2211 Gateway Settings Worksheet

Print Table 5, and record your personalized settings for configuring the MM2211 Gateway. Enter the security settings you recorded in Table 4, "Wireless Network Settings Worksheet," on page 20.

Remember—*If the MM2211 Gateway's device settings do not match the Mesh Networks Router settings, the MM2211 Gateway will not be able to find your network.*

Store this information in a safe place.

Table 5—MM2211 Gateway Default and User Settings Worksheet

Item	Default Setting	Your Setting
User Name	**admin**	_____
Password	**password**	_____
IP Address	**192.168.1.1**	_____
Subnet Mask	**255.255.255.0**	_____
SSID	V54-XXXX	_____
Wireless Mode	802.11g & b	_____
Security	Disabled	_____

Ruckus Wireless Web Interface Menus

The Ruckus Wireless Web Interface menus are located on the left-hand navigation pane. To select a particular menu, simply click on the menu link.

Common Buttons

The Ruckus Wireless Web Interface screens contain the following menu buttons (Table 6):

Table 6—Wireless Web Interface Menu Buttons

Button	Action
Logout	Logs out the current session.
Restore	Restores the last executed configuration change.
Update	Saves the new configuration.
Next	Progresses to the next menu. Only found in the Configuration menus.
Back	Reverts to the previous menu. Only found in the Configuration menus.

Air Quality Indicator

The Air Quality indicator icon shows the current state of your Wireless connection. Air Quality is measured by the Received Signal Strength Indication (RSSI) value, which is a measurement of the wireless signal strength. A high RSSI value usually means that the wireless connection is stable, and quality data transmission can be achieved.

The Air Quality Indicator examines the environment that surrounds a Ruckus Wireless, Inc. MM2211 Gateway, and determines the amount of interference in the environment. The Radio Frequency (RF) side of a wireless device is a combination of a receiver and a transmitter. Both receiver and transmitter provide feedback as they operate. The Air Quality indicator bases its evaluation on the Received Signal Strength Indication (RSSI) that is returned as part of the 802.11 transmission acknowledgement. As the adapter receives an 802.11 packet, it sends the RSSI value to the remote AP.

Thumb Up: Good air quality. The environment supports a quality data transmission.

Thumb sideways: Marginal data transmission strength. The current environment *may* support data transmission, but it is possible that the data transmission quality may be marginal.

Thumb down: Low data transmission strength. The current environment does not support acceptable data transmission.

Configuring the MM2211 Gateway

This section describes the tasks and screens used to customize the MM2211 Gateway configuration to run on your wireless network.

Review the following topics before you change any system configuration settings:

- "Connecting to the MM2211 Gateway" on page 15
- "Accessing the Web Interface" on page 17.
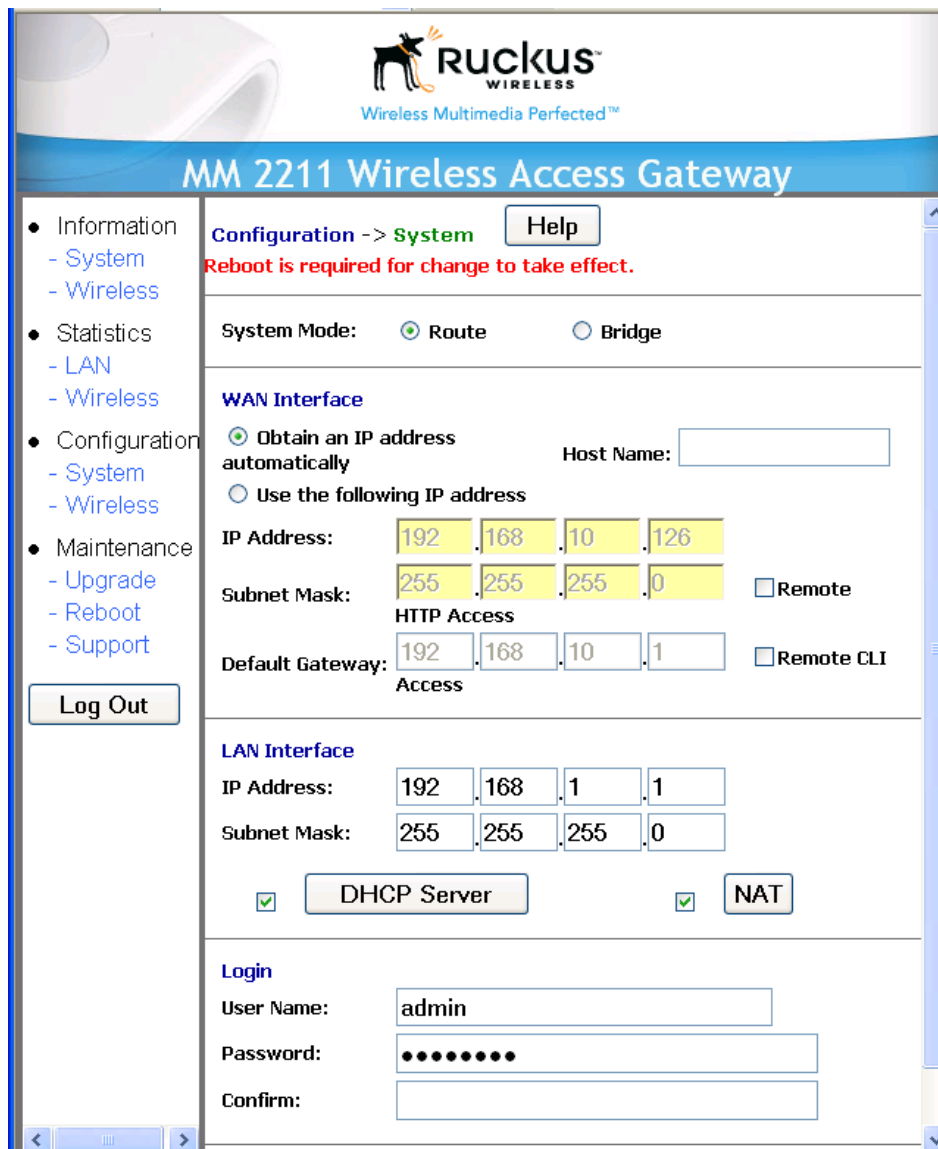
System Configuration

Table 5, "MM2211 Gateway Default and User Settings Worksheet," on page 21 shows the default settings used to login to the device.

A minimum set of configurations is required to put the MM2211 Gateway into operational mode. The system provides the default settings for these configuration items. You should change the default settings where necessary to match your own wireless network's configuration, and to protect your privacy.

A system reboot is required for configuration changes to take effect. Follow the following steps to configure the MM2211 Gateway:

1. Connect to the MM2211 adapter by following the instructions in "Connecting to the MM2211 Gateway" on page 15.

2. Choose **Configuration->System**. The window of Figure 5 appears.

Figure 5—*System Configuration—Route Mode*

Figure 6—*System Configuration—Bridge Mode*

The System->Configuration window allows you to configure system mode—either Route or Bridge. In addition, this window allows you to configure IP address assignment and to change the username and password to access the device.

Route mode provides the capability to perform NAT (network address translation) of the traffic from the Internet (WAN Interface) to the local interface. Route mode allows home users to hide the MM2211 IP address from the Internet. Using Route mode, multiple devices can be connected behind the Metro Wireless Access Gateway.

Bridge mode allows the Wireless Access Gateway to act in Layer 2 (or bridge) mode. When the bridge mode is selected, the home PC's IP address will not be changed as it communicates with the Metro Mesh node. The Wireless Access Gateway will use the MAC address of the home PC as it sends the packet to the Metro Mesh Node. This mode is sometimes referring to as *cloning* mode. Using the Bridge mode, only a single device can be connected behind the Metro Wireless Access Gateway.

3. Choose the system mode, either *Route* or *Bridge*.

4. Enter your configuration changes in the appropriate fields.

5. Click the **Update** button to save your settings.

6. Click **Reboot** to reboot the device so configuration changes can take effect.

> ⚠ *CAUTION:—You must click the **Update** button to save any configuration changes. The Ruckus Wireless Web Interface will timeout after 5 minutes of inactivity. If you let the system time out before clicking the **Update** button, any changes you made will be lost.*

> ⚠ *CAUTION:—If, after having changed any default settings, you have forgotten what the new settings are, you may not be able to login to the MM2211 Gateway. To regain access to the MM2211 Gateway, you must reset the device to its factory default settings. Hold the button down for more than 8 seconds, then release. The Air Quality indicator will go off and then back on.*

Customizing the System Configuration

It is recommended that you customize the username and password so that you can control who can gain administrative access to the MM2211 Gateway. We recommend that you do not change the IP address (LAN) of the MM2211 Gateway. The MM2211 Gateway has DHCP enabled by default, and provides network address translation and security functionality to your home PC. Refer to Table 7 for details on each field.

Table 7—System Configuration—Route Mode

Field	Description
WAN Interface	The selection criteria for WAN interface determine how the Metro Wireless Access Gateway receives its IP address assignment on the WAN interface. Selecting Obtain an IP address automatically will allow the Wireless Access Gateway to get a dynamically assigned IP address from the Metro Mesh node (or the DHCP server behind the Metro Mesh node). Use the following IP address selection to statically configure an IP address to the Wireless Access Gateway.
IP Address/Subnet Mask	The IP Address is the internal IP address of the device. You must configure the IP Address and Subnet Mask for managing this device. The default setting of the IP Address and Subnet Mask is as follows: **Bridge Mode**: 192.168.0.254 255.255.255.0 **Route Mode**: 192.168.1.1 255.255.255.0
Default Gateway	This is the IP address of the default gateway. This is normally provided by your ISP (Internet Service Provider).

Table 7—System Configuration—Route Mode (Continued)

Field	Description
LAN Interface	LAN interface configuration provides the selection of the IP address assignment from the Local Area Network. This is the IP address that the home users will use to access the Web Interface.
DHCP Server	Selecting the DHCP Server will allow the Metro Wireless Access Gateway to act as a DHCP server to assign IP address to PC's connected to the Wireless Access Gateway.
NAT	Selecting NAT (Network Address Translation) will perform all address translation from the internal IP address to external IP address.
User Name	The user name. The default user name is **admin**. If you change the user name, make sure to write it down for future reference.
Password / Confirm	The user password. The default is **password**. If you change the password, make sure to write it down for future reference.

Configuring the Wireless Interface

It is recommended that you consult with your service provider to understand the wireless settings. Before changing any settings in the Wireless configuration menu, make sure you have recorded and verified the information in the following worksheets:

- "Wireless Network Settings Worksheet" on page 20
- "MM2211 Gateway Default and User Settings Worksheet" on page 21.

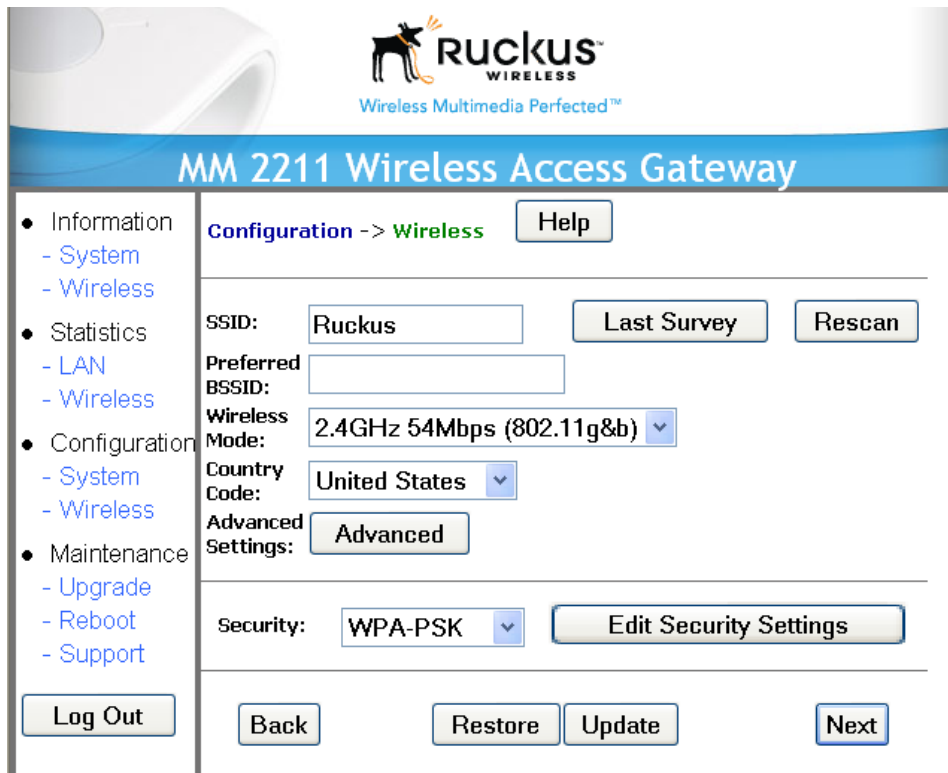1. After connecting to the MM2211 Gateway, choose **Configuration->Wireless**. The window of Figure 7 appears.

***Figure 7**—Wireless Interface Configuration*

2. Enter the preferred BSSID (optional).
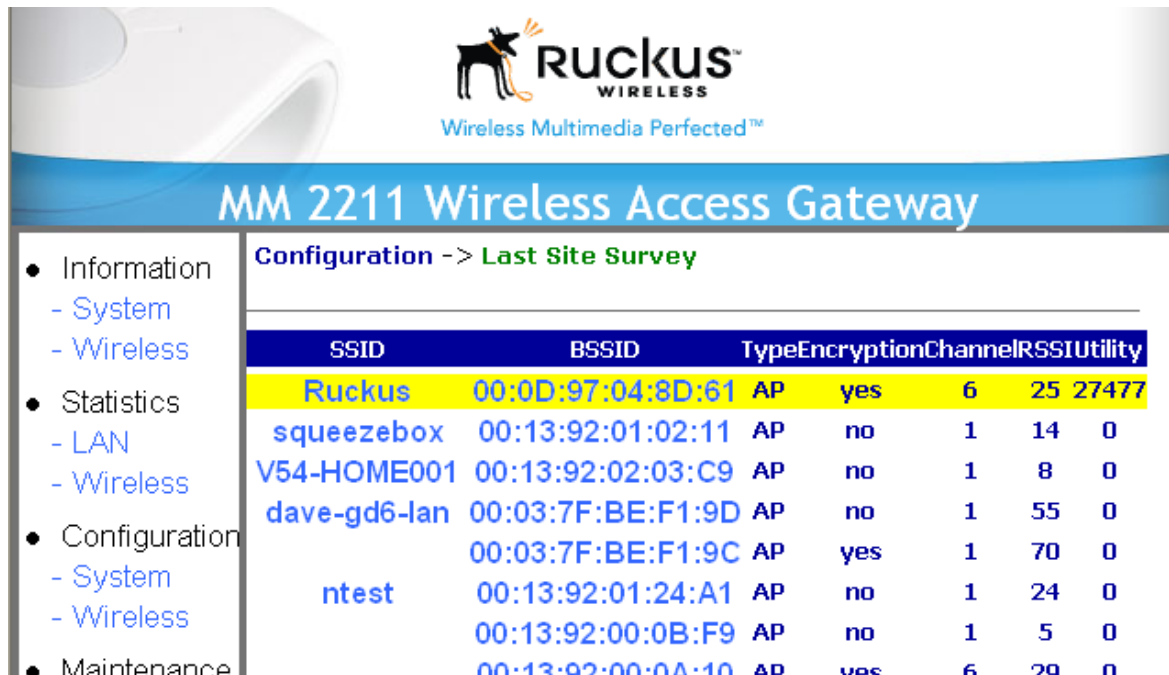3. Click **Last Survey**. The Last Survey window (Figure 8) appears.

***Figure 8**—Last Survey Window*

4. Move your mouse to the desired entry in the window. The entry text will change color. Click to select.

5. Fill in the parameters as described in Table 8.

Table 8—Wireless Interface Configuration

Field	Description
SSID	The SSID (Service Set IDentifier) is the name of the wireless network. The default SSID is `V54`, but you should change your SSID to that given by your Metro ISP provider. The SSID can consist of up to 32 characters.
Preferred BSSID	The preferred BSSID allows you to select the specific Metro node to which you want to associate. For example, an SSID of Ruckus has two nodes, with each node having a unique BSSID
Wireless mode	The wireless mode options are: • **2.4GHz 54Mbps (802.11g&b)** - allows both 802.11g- and 802.11b-compliant devices to join the network. This is the default setting.

Table 8—Wireless Interface Configuration (Continued)

Field	Description
Country Code	Sets your country or region code. Selecting the incorrect country or region may result in violation of applicable law. The selectable countries or regions are United States, Europe, Hong Kong, and Japan. **NOTE –** For MM2211 Gateways shipped in the United States, the country code cannot be modified. The country code is pre-defined for **United States** only.
Advanced Settings	This button provides access to the advanced wireless settings. Advanced wireless settings are for advanced configuration or testing purposes only. Changing the advanced settings may negatively affect the operation of the MM2211 Gateway and is *not recommended*.
Security	The wireless security options are: • **Disabled**: This setting disables all encryption, so traffic is sent in the clear. This setting is not recommended. • **WEP**: This setting enables Wired Equivalent Privacy. WEP Shared Key authentication and WEP data encryption provides sufficient security in most cases. • **WPA-PSK:** Wi-Fi Protected Access, Pre-Shared Key (WPA-PSK). Each packet of information is encrypted with a different key. Provides very strong security, but may not be supported on older systems. • **WPA-802.1X**: Extensible Authentication Protocol (EAP) using Tunneled Transport Layer Security (TTLS).
Edit Security Setting	Click this button to edit the security setting of WEP keys or the WPA-PSK passphrase.

6. When you are finished, click **Update** to save these settings.

Advanced Wireless Configuration

The Advanced Wireless Configuration menu is preconfigured with the optimum settings. Changing the advanced settings may negatively affect the MM2211 Gateway's operation, or completely disable it. For best results, leave the Advanced settings at their default values and do not change these settings unless directed by your technical support personnel.

NOTE – If you have modified the advanced settings and wish to revert to the original settings, you can restore the settings by clicking the **Restore** button, as long as you have not already clicked the **Update** Button.

1. After connecting to the MM2211 Gateway, choose **Configuration->Wireless**. Then click **Advanced**. The window of Figure 9 appears.
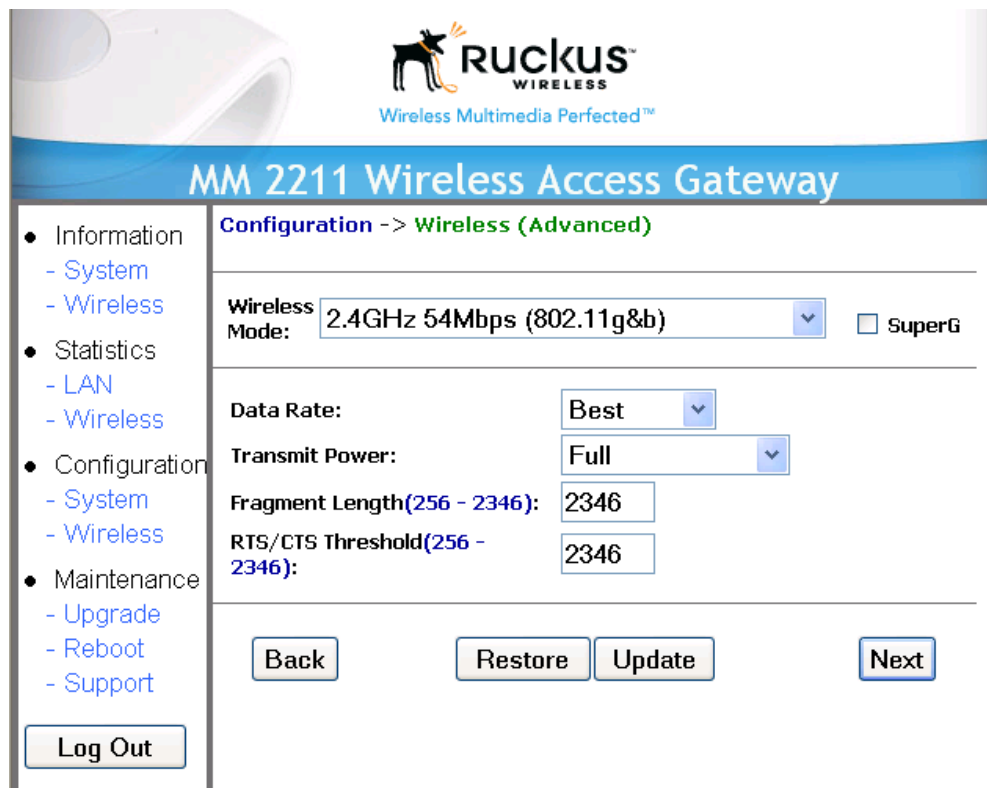
Figure 9—Advanced Wireless Configuration

Table 9 shows the Advanced Wireless Configuration parameters.

Table 9—Advanced Wireless Configuration Parameters

Field	Description
Wireless Mode	Sets the wireless mode for the MM2211 Gateway. The wireless mode determines the wireless speed of devices that are allowed to associate to the MM2211 Gateway. Options are: • 802.11g&b: stations running at either 802.11g (2.4GHz, 54Mbps) or 802.11b (2.4GHz 11Mbps) can associate to the MM2211 Gateway. This is the default setting. • 2.4GHz 54Mbps (802.11g only) • 2.4 GHz Auto 108Mbps (802.11g Turbo) • 2.4 GHz 108 Mbps Only (802.11g Turbo)
Super G	Enables Super G. Super G allows communications with the remote Access Point in "Super G" mode (implementing frame-bursting and compression). This is not supported in many metro applications. It is recommended to leave this off unless informed otherwise by your service provider.

Table 9—Advanced Wireless Configuration Parameters (Continued)

Field	Description
Data Rate	Select the desired data rate from the drop-down menu. The default is **Best**, which means the system will adjust the data rate automatically.
Transmit Power	Select the desired Adapter transmit power from the drop-down menu. We recommend that you use the default power, *Full*.
	The options are:
	• Full
	• Half (-3 dB)
	• Quarter (-6 dB)
	• Eighth (-9 dB)
	• Minimum
	The default is **Full**.
Fragment Length	The fragment length. The range is between 256 and 2346 bytes. The default is **2346**.
	The MM2211 Gateway uses fragmentation to divide 802.11 frames into smaller fragments which are sent separately to the destination. Only unicast frames can be fragmented. The fragment length can be between 256-2346 bytes. If the data that the MM2211 Gateway is transmitting is larger than the threshold, it will trigger the fragmentation function. If the packet size is equal to or less than the threshold, the gateway will not use fragmentation. In a good wireless environment, the larger the fragment, the more efficient the network operates. In a noisy environment, the fragment length should be adjusted to a smaller size to minimize retransmission and increase the reliability of the transmission.
RTS/CTS Threshold	The RTS-CTS threshold range. The range is between 256 and 2346. The default is **2346**.
	The RTS-CTS threshold is a value that determines at what frame length the request-to-send/clear-to-send (RTS-CTS) function is triggered. By default, this threshold is set at its highest value. A lower threshold value means that the RTS-CTS function is triggered for smaller frame lengths.
	A lower threshold may be necessary in environments with excessive signal noise or hidden nodes; but this may result in some performance degradation.

2. Click **Update** when you are done.

Configuring WEP Security

1. Click **Configuration** ->**Wireless** in the left-hand navigation pane. The window of Figure 7 appears.

2. Select **WEP** in the **Security** drop-down menu.

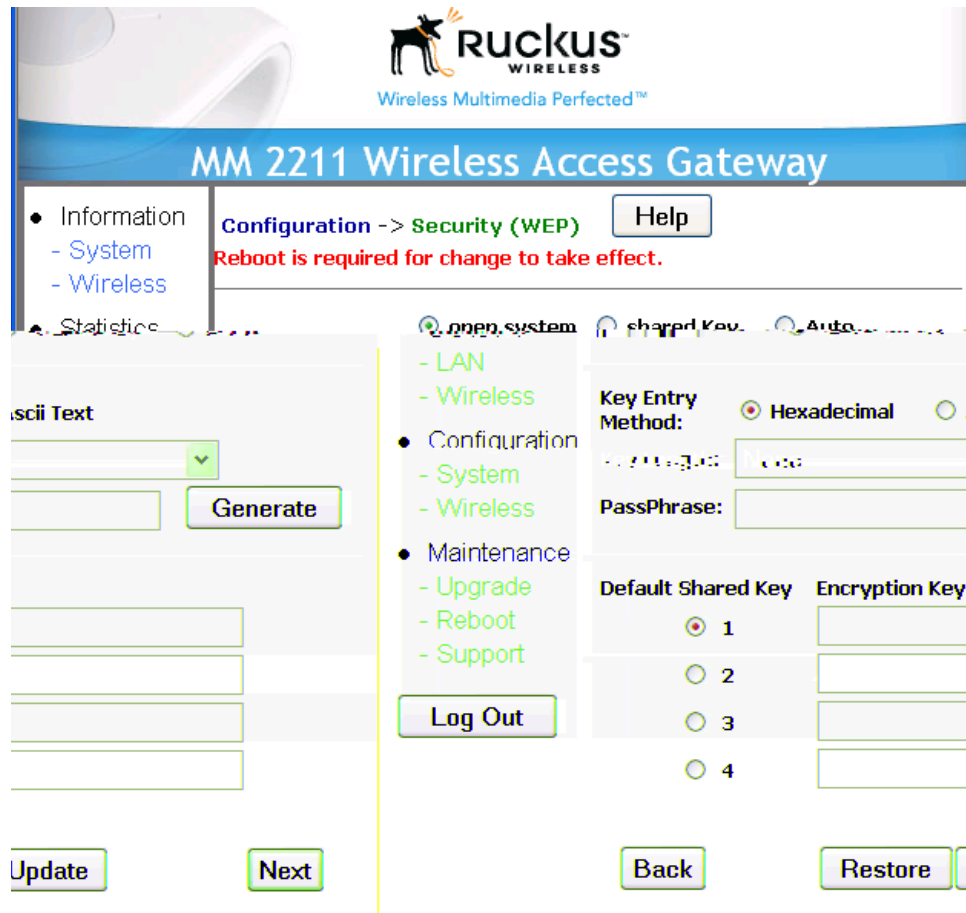**3.** Click the **Edit Security Settings** button.TheWEP Configuration window of Figure 10 appears.

Figure 10—WEP Configuration Window

Table 10 explains the WEP Configuration parameters.

Table 10—WEP Configuration

Field	Description
Authentication	WEP allows three authentication options: *open system*, *shared key,* or *automatic* selection of authentication method. *Shared key* authentication adds another layer of security by requiring that the MM2211 Gateway supply a shared key first to authenticate to the Mesh Networks Outdoor Router, and then supply the same shared key for encrypting and decrypting data. Choosing *Auto*, automatically selects the authentication mode depending on the method used by the remote AP.
Key Entry Method	You can choose either Hexadecimal or ASCII as the entry method
Auto	Configuration is performed automatically.

Table 10—WEP Configuration (Continued)

Field	Description
PassPhrase	The MM2211 Gateway supports automatic generation of four keys from a passphrase. Make sure that the passphrase is the same as the passphrase used on the remote AP. Enter a word or group of printable characters in the Passphrase box and click **Generate**. The passphrase is case sensitive; e.g. **MediaFlex** is not the same as **MEDIAFLEX**. The four key boxes will be automatically populated with key values. Click the **Update** button to save your settings.
Confirm	Confirm your passphrase
Default Shared Key/Encryption Key	You can create an encryption key in either of two ways. If you enter a word or group of printable characters in the Passphrase box and click Generate, the four encryption keys will be populated. Or you can edit any of the encryption keys to match a pre-existing key.

Configuring WPA PSK

WPA PSK configuration menu allows automatic key generation based on a single passphrase. WPA PSK provides very strong security.

If you configure the MM2211 Gateway with WPA-PSK, you can only communicate with another AP that is is setup with the same WPA-PSK passphrase.

1. Click the **Configuration -> Wireless** link in the left-hand navigation pane (Figure 7).
2. Select **WPA-PSK** in the **Security** drop-down menu.
3. Click the **Edit Security Settings** button.The WPA Configuration appears (Figure 11).
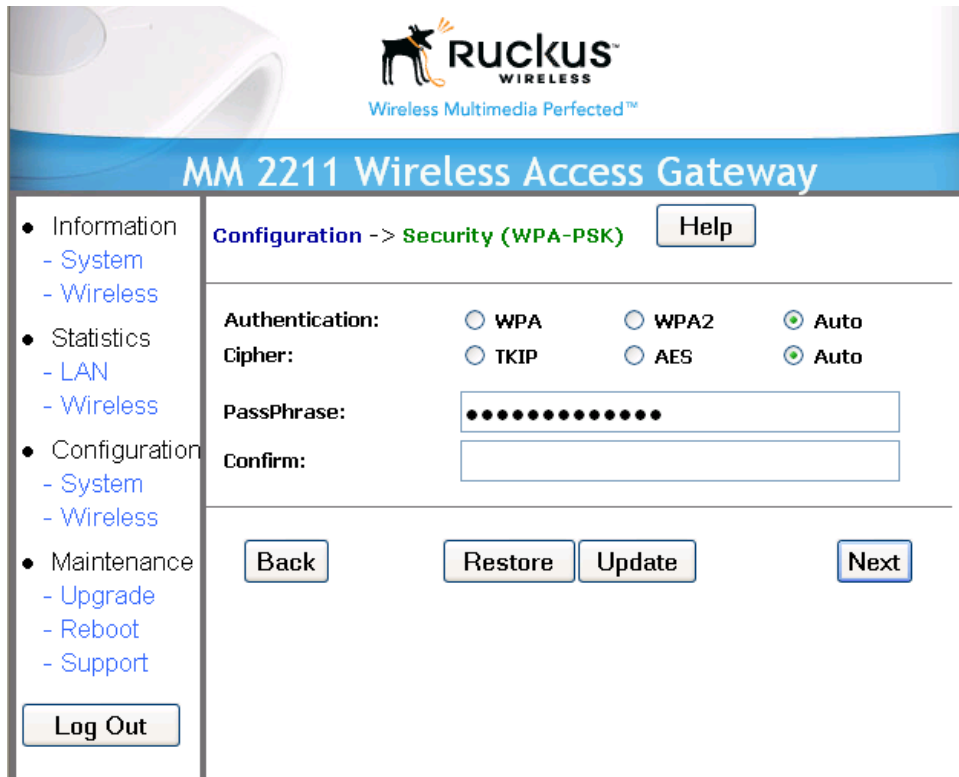
Figure 11—WPA Configuration

Table 11 explains the WPA Configuration parameters and a description of the Authentication and Cipher choices.

Table 11—WPA Configuration

Field	Description
WPA	Wi-Fi protected access using Temporal Key Integrity Protocol (TKIP)
WPA2	Wi-Fi protected access using the Advanced Encryption Standard (AES)
Authentication	Choices are WPA, WPA2 or Auto.
Cipher	Choices are TKIP, AES, or Auto.
PassPhrase / Confirm	Enter a passphrase and enter it again in the **Confirm** field.

4. In the **Configuration ->Security (WPA-PSK)** menu, enter a passphrase and enter it again in the **Confirm** field.

5. Click the **Update** button to save your settings.

Table 12—Phase 2 Choices

Field	Description
PAP	Password Authentication Protocol. One user sends the other a user name and password for authentication.
CHAP	Challenge Handshake Authentication Protocol. One user sends the other a random number or challenge. The second hashes his copy and sends it to back to the first. The first user hashes its copy of the second users response. If the hashes match, the password is correct.
MSCHAP	Microsoft Challenge Handshake Authentication Protocol.
MSCHAP/2	An updated version of MSCHAP.
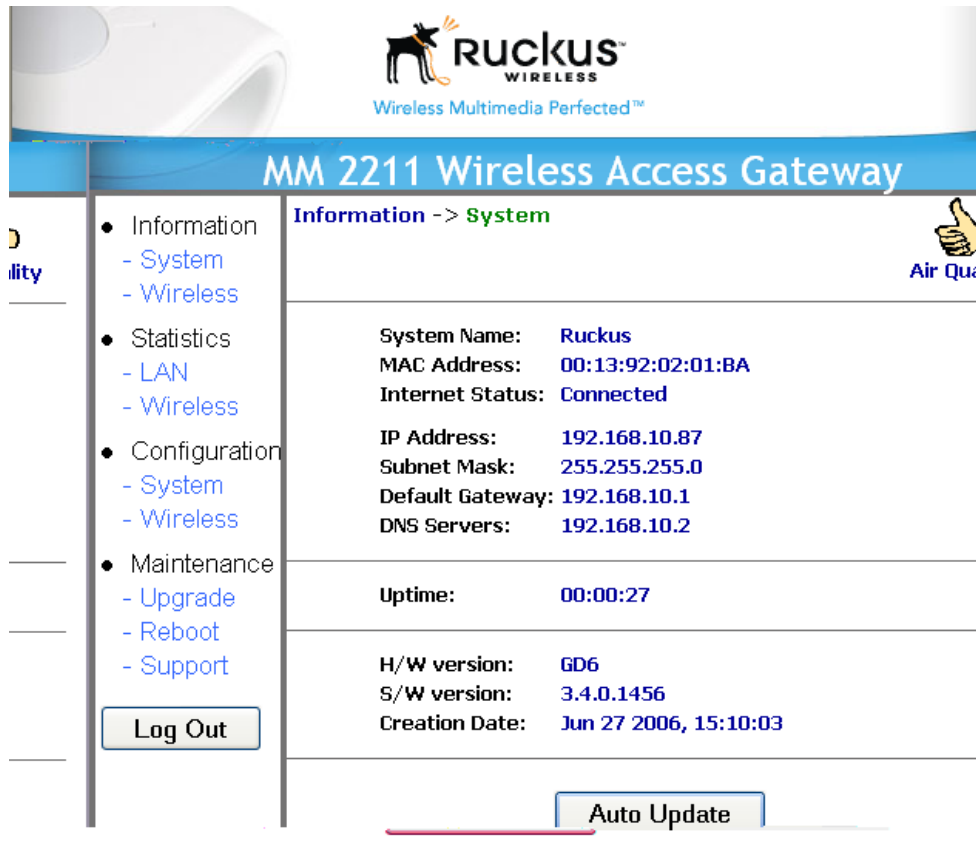
7. Click the **Update** button to save your settings.

Viewing System Information

The Information Screens provide information about the MM2211 Gateway settings.

System Information

The System Information screen is the first screen to appear once you login to the MM2211 Gateway. Figure 13 shows the System Information window.

Figure 13—System Information Window

Table 13 explains the System Information Parameters.

**Table 13—System Information Parameters**

Field	Description
System Name	The local name for the MM2211 Gateway, if the device is configured as a router.
MAC Address	The MAC address of the MM2211 Gateway, or the station behind the adapter, if the device is configured in bridge mode.
Internet Status	Connected or Disconnected. The MM2211 verifies the internet access by checking to see if the gateway is up or down.
IP Address	The IP address of the MM2211 Gateway.
Subnet Mask	The subnet mask of the MM2211 Gateway.
Default Gateway	The gateway IP address
DNS Servers	The IP addresses of any domain name servers.

Table 13—System Information Parameters (Continued)

Field	Description
Uptime	The system uptime since last reboot, displayed in HH:MM:SS (hours, minutes, seconds).
H/W Version	The hardware revision.
S/W Version	The firmware version that is currently operating.
Creation Date	The date/time that the firmware was created.

Viewing Wireless Information

The Wireless information menu shows the current wireless configurations for the MM2211 Gateway. To view this window, click **Information->Wireless** from any window. Figure 14 shows the Wireless Information Window.
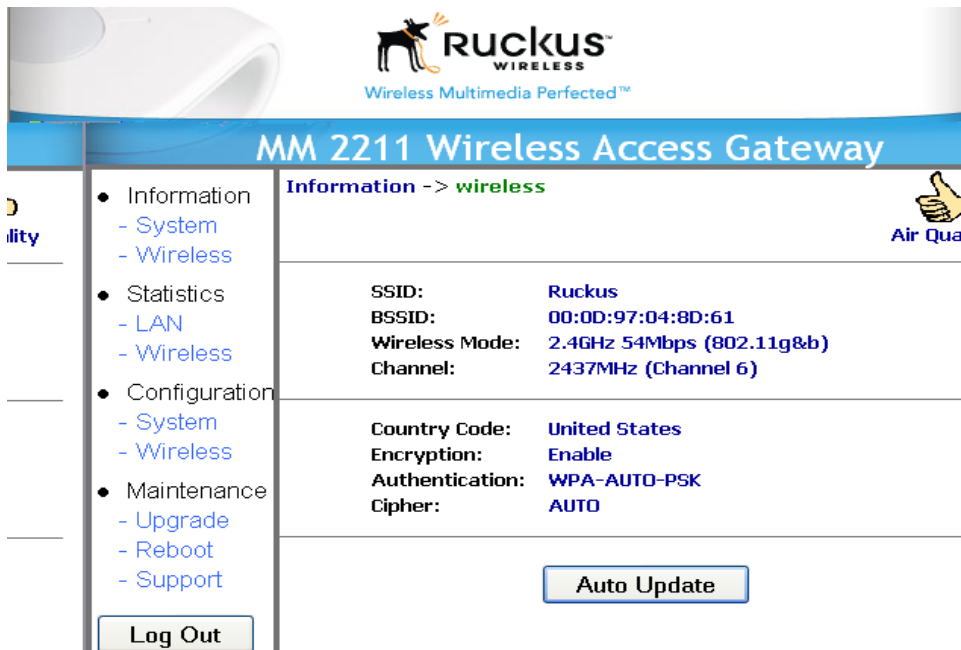
Figure 14—*Wireless Information Window*

Table 14 shows the Wireless Information Window parameters.

Table 14—Wireless Information Window Parameters

Field	Description
SSID	The SSID (Service Set Identifier) is the name of the wireless network.
BSSID	The BSSID is the MAC address of the Metro Mesh Outdoor Router to which the MM2211 Gateway is associated.

Table 14—Wireless Information Window Parameters (Continued)

Field	Description
Wireless Mode	The wireless mode, such as **2.4 GHz 54Mbps (802.11b/g)**
Channel	The wireless channel number and operating frequency in MHz.
Country code	The country in which the MM2211 Gateway is operating.The country code will automatically select the Channels available for that country.
Encryption	Enabled or Disabled
Authentication	Choices are WPA, WPA2 or Auto.
Cipher	Choices are TKIP, AES, or Auto.

Viewing Statistics

The Statistics Screens provide statistics for a Local Area Network (LAN) interface, the wireless interface and wireless stations.

Viewing LAN Interface Statistics

The LAN Interface statistics windows show information about packets traversing the LAN connected to the MM2211 Gateway. To view the LAN interface statistics, choose **Statistics->LAN** from any window. Figure 15 shows the LAN Statistics Window.
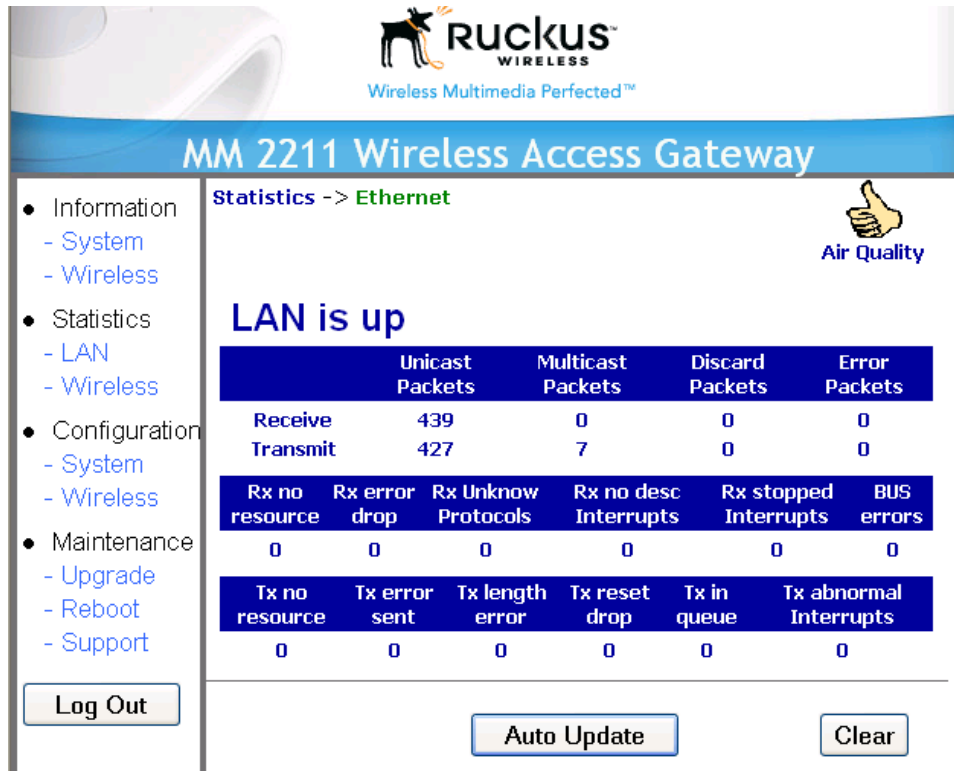
***Figure 15**—LAN Statistics Window*

Table 15 explains the LAN Statistics window parameters.

Table 15—LAN Statistics Window Parameters

Field	Description
Unicast Packets	The total number of unicast packets received or transmitted by the interface.
Multicast Packets	The total number of multicast packets received or transmitted by the interface.
Discard Packets	The total number of received packets that were discarded by the interface.
Error Packets	The total number of error packets received or transmitted by the interface.
Rx No Resource	The number of received packets that are discarded by the interface due to no system resources.
Rx Error Drop	The number of received packets that are discarded by the interface due to a hardware error.

Table 15—LAN Statistics Window Parameters (Continued)

Field	Description
Rx Unknown Protocols	The number of received packets that are discarded by the interface due to an unknown protocol.
RX No Desc Interrupts	The number of received packets that are discarded by the interface due to no descriptor interrupt.
RX Stopped Interrupts	The number of received packets that are discarded by the interface due to stopped interrupts.
BUS Error	The number of received packets that are discarded by the interface due to a BUS error.
Tx No Resource	The number of transmitted packets that are discarded by the interface due to no system resources.
Tx Error Sent	The number of transmitted packets that are discarded by the interface due to a hardware error.
Tx Length error	The number of transmitted packets that are discarded by the interface due to a length error.
Tx Reset Drop	The number of transmitted packets that are discarded by the interface due to reset drop.
Tx In Queue	The number of transmitted packets that are discarded by the interface due to being in the queue.
Tx Abnormal Interrupts	The number of transmitted packets that are discarded by the interface due to abnormal interrupts.

Viewing Wireless Statistics

The Wireless statistics menu shows the link, traffic, and security settings for the MM2211 Gateway. To view this menu, choose **Statistics->Wireless**. The Wireless Statistics Window of Figure 16 appears. At the top of this menu, MM2211 Gateway's MAC address will display as either **joined** or **disconnected** to the remote AP.

Joined means that the MM2211 is associated with the remote AP; disconnected means that the MM2211 is not associated with the remote AP.

Figure 16—Wireless Statistics

1. Click the **Auto Update** button to receive periodic updates to these statistics. The button will then display as **Stop Update**.

2. Click the **Stop Update** button if you do not wish to receive periodic updates.

Table 16 shows the Wireless Statistics parameters.

Table 16—Wireless Statistics

Field	Description
Good Packets	The total number of good packets received or transmitted by the interface.
Retries	The total number of packets that were retried.
Discards DMA Error	The number of discarded packets
Phy Rate (Mbps)	The data rate of the PHY in Mbps.

Table 16—Wireless Statistics (Continued)

Field	Description
Throughput Estimate (Mbps)	The theoretically possible receive or transmit throughput in megabits per second.
PER (%)	The PHY error rate expressed as a percent.
Estimated SNR (dB)	The estimated signal to noise ratio in dB.
Discards CRC Errors	The number of packets with CRC error received or transmitted by the interface.
Noise Floor (dB)	The value of the noise floor, expressed in dB.

Updating the Firmware

This menu provides a utility for updating the MM2211 Gateway's firmware. A firmware update may be necessary or desirable to add new features, important fixes or enhancements to the MM2211 Gateway.

The MM2211 is provided with an automatic firmware upgrade feature. This feature checks to verify that you have the latest firmware when you reboot the MM2211, or at an interval you set even if you do not reboot. The automatic firmware upgrade is the default option. You may wish to disable the automatic firmware upgrade, and select manual firmware upgrade.

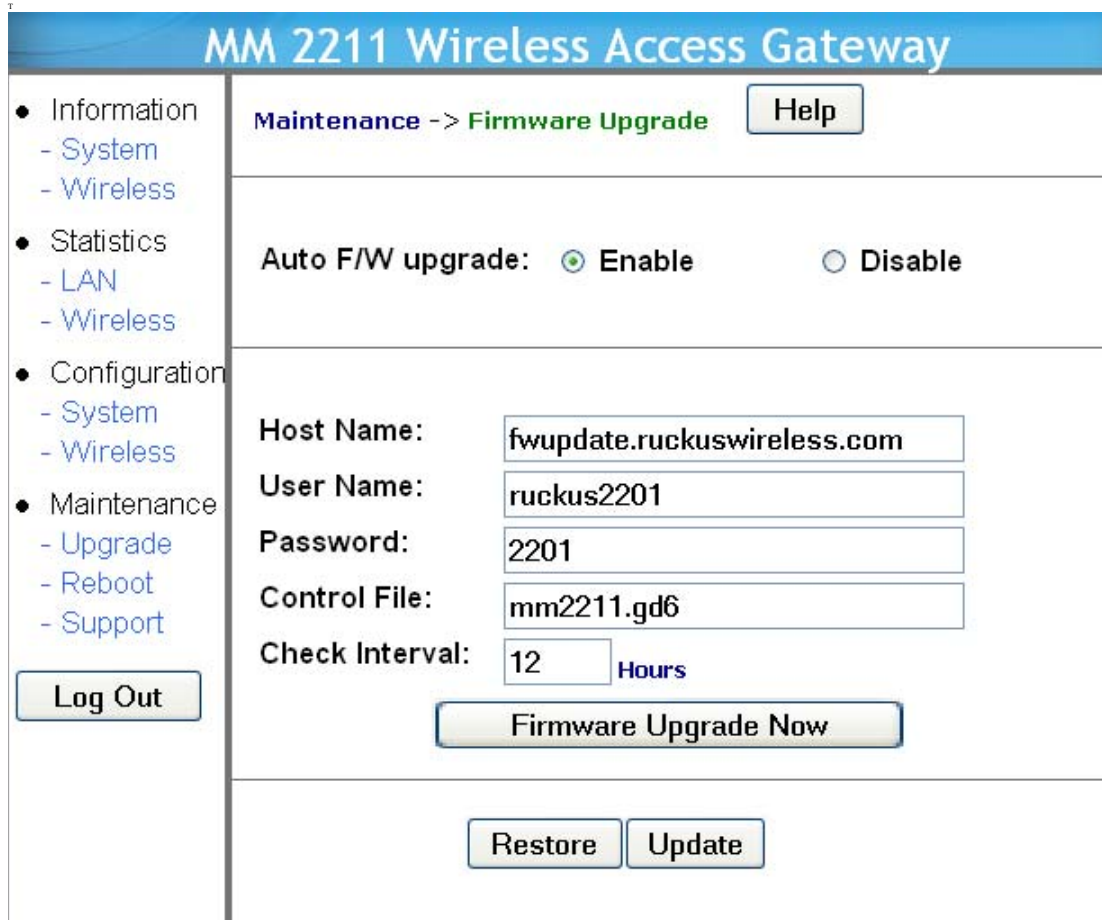**1.** In the Ruckus Wireless Web Interface, click the **Maintenance->Upgrade** menu. The window of Figure 17 appears.

Figure 17—*Updating the Firmware*

Automatic Firmware Upgrade

The Host Name, User Name, and Password shown in the window of Figure 17 have been preconfigured to automatically access Ruckus Wireless's firmware update website. You can alternatively change these parameters to access a different firmware upgrade website.

You can perform an immediate firmware upgrade by clicking **Firmware Upgrade Now**. The MM2211 will proceed with a firmware upgrade at the host specified.

The default for checking for new updates is 12 hours, as shown in the Check Interval box. You can set this to a longer or shorter interval as required.

1. If you are satisfied with the automatic firmware upgrade parameters, click **Update**. The system will update the firmware as required.
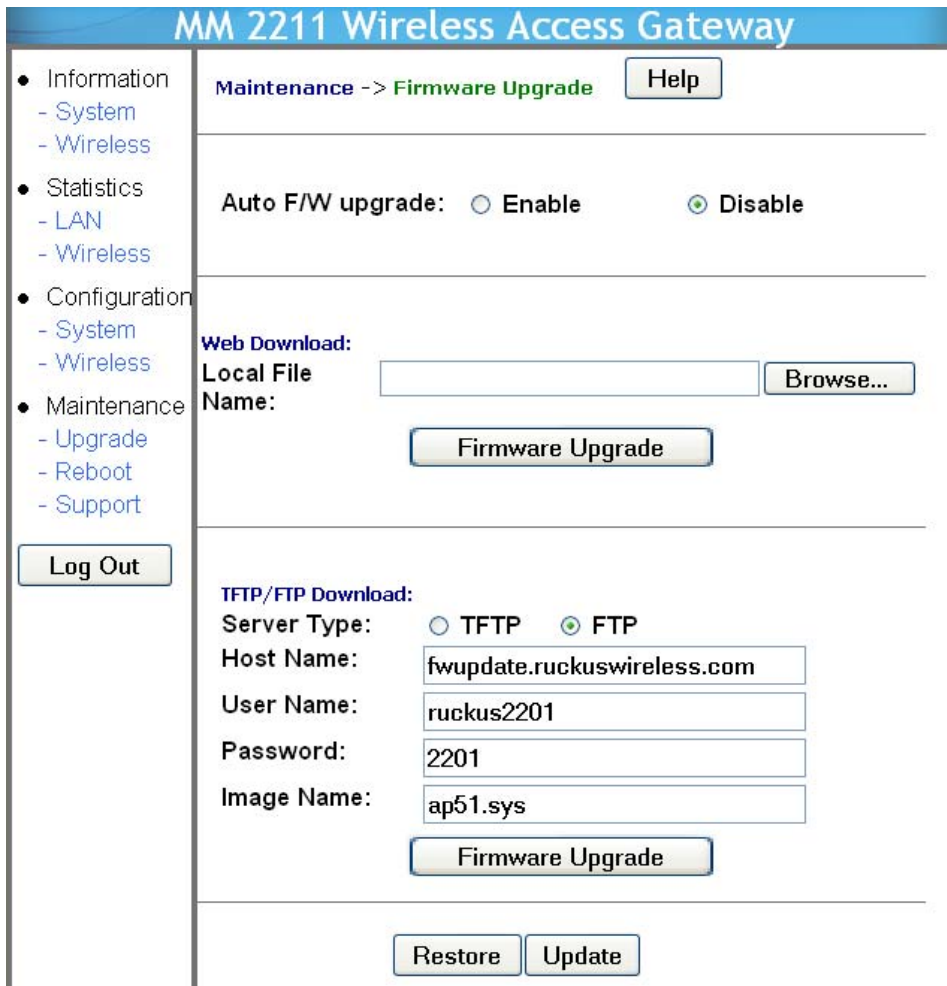
Manual Firmware Upgrade

Contact your service provider for more information about Web sites or TFTP/FTP sites used to store firmware images for the MM2211 Gateway.

CAUTION:—*If you have recently made configuration changes to the MM2211 Gateway, make sure to reboot the system (see "Rebooting the System" on page 50) first so that your changes are preserved. Then update the firmware.*

To choose the manual firmware upgrade option, proceed as follows:

1. In the Auto F/W upgrade box of Figure 17, check **Disable**.
2. The window of Figure 18 appears

Figure 18—*Manual Firmware Upgrade Window*

To download a firmware image from a Web site and use it to update the firmware on the MM2211 Gateway:

1. Point your browser to the Web site where the MM2211 Gateway's firmware is stored, and download the firmware image to a folder on your hard drive. Note the location of the downloaded image.

Table 17 describes the Updating the Firmware parameters.

Table 17—Updating the Firmware

Field	Description
Web Download	If you have downloaded a Firmware image from a Web site and stored it locally on your PC, you can click the **Browse...** button to select the image. The path to the image will appear in the **Local File Name:** field. Click **Firmware Upgrade**, located below the **Local File Name** field.
TFTP/FTP Download	Allows you to use a TFTP or FTP server to download a firmware image. • **Host Name:** enter the IP address of the server. • **User Name:** enter the User Name that is used to access to the specified server. This is required only for an FTP server • **Password:** enter the Password that is used to access to the specified server. This is required only for an FTP server. • **Image Name:** enter the filename of the firmware image on the TFTP or FTP server. Click **Firmware Upgrade**, located below **Image Name** field.

2. Click the **Browse...** button to locate and select the firmware image.

3. Click the **Firmware Upgrade** button to perform the update.

4. The window of Figure 19 appears.

***Figure 19**—Upgrading Software in Process*

5. If the firmware has updated successfully, a green check mark will appear (Figure 20).

ton.

Figure 20—Successful Image Upgrade

6. Click the **Reboot** button.

7. If the firmware did not update, a **Failed: file type** error message will appear.

A file type error indicates that the firmware image may be corrupt or invalid. Try downloading the firmware image again, and repeat the above steps.

TFTP or FTP Download

To specify a specific trivial file transfer protocol (TFTP) or File Transfer Protocol (FTP) server from which to download a firmware image:

1. Ensure that the MM2211 has Internet access to reach the TFTP or FTP server that contains the image.

2. Choose the download method by selecting either the **TFTP** or **FTP** button.

3. Enter the IP address or Hostname of the server.

4. For FTP only: Enter the **User Name** and **Password** for the server.

5. Enter the name of the firmware image.

6.

8. If the firmware did not update, a **Failed: file type** error message will appear.

A file type error indicates that the firmware image may be corrupt or invalid. Check the TFTP/FTP server address and the firmware image name. Then try downloading the firmware image again, and repeat the above steps.

9. You must now reboot the system.

Rebooting the System

You must reboot the system if you want your configuration changes to take effect.Two types of reboot are provided:

The **Reboot** button re-starts the system. All the configurations that have been saved are preserved through the reboot. Rebooting is necessary in order to make your configuration changes permanent.

- If the system times out and you have to re-login before setting the reboot, your configuration changes will be saved, as long as you have already clicked the Update button to save the current configuration.

- If you have powered down or logged out of the MM2211 Gateway before clicking the **Update** button and the **Reboot** button, your configuration changes will be lost.

The **Reboot to Factory Default** button restarts the system with the factory default configurations. All previous configurations will be lost.

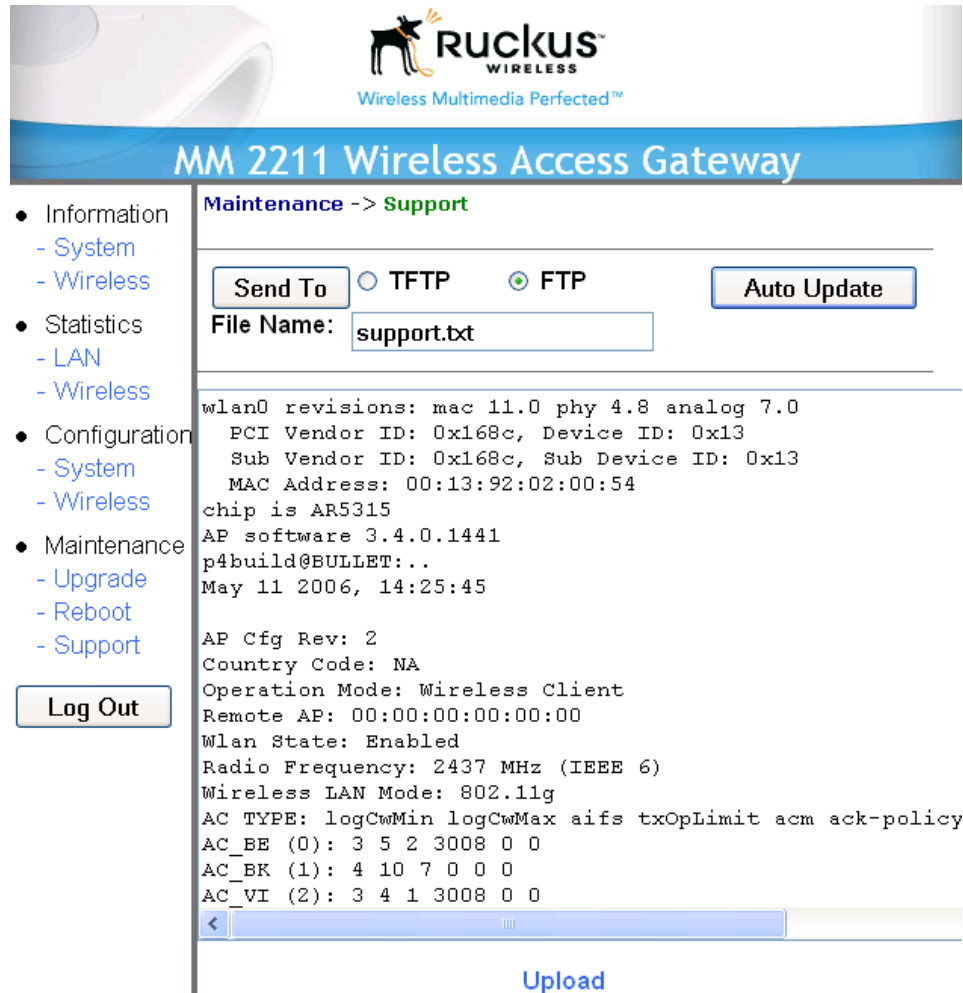**1.** To reboot for either type, click **Maintenance->Reboot** from any window. The window of Figure 21 appears.

***Figure 21**—Reboot Menu*

During a reboot, the antenna LEDs on the top of the MM2211 Gateway will momentarily go out, then light up again.

Taking a System Support Snapshot

The Support menu enables you to take a system snapshot for further analysis and troubleshooting. The system snapshot can be sent and saved to a TFTP or FTP server for analysis by a technical support engineer.

1. To view the support menu, choose **Maintenance->Support** from any window. The Support Menu appears (Figure 22).

Figure 22—*Support Menu*

Table 18 describes the support menu parameters.

Table 18—Support Menu

Field	Description
Send To	Select the server type: TFTP or FTP.
File Name	Specify the file name for the system snapshot that is to be saved on a TFTP or FTP server.

NOTE – If you have not yet configured the TFTP or FTP server, click the **Maintenance->Upgrade** link.

2. In the **Firmware->Upgrade** menu, enter the TFTP or FTP server information. The same server is used for both upgrading the firmware and uploading the system snapshot.

Your service provider or technical support contact should provide you with information for configuring the TFTP or FTP server.

3. Click on the **Refresh** button to get the current system snapshot.

4. Click on the **Send To** button to send the `support.txt` file to the TFTP or FTP server. You can set the address for the TFTP or FTP server in the **Firmware Update** menu.

5. Click the **Upload** link at the bottom of the page to upload to the specified server.

Appendix A: Technical Specifications

Physical Characteristics

	MM2211 Wireless Broadband Gateway:
	5V-18V 10W
	External power adapter:
Power requirements	Unifive Technology Co LTD, Model US300520, Input 100-240V AC, Output 5V DC 2A, UL Listed
	DVE, Model DSA-031F-12 UK 12, Input 100-240V AC, Output 12V DC 1A, TUV Certified
	DVE, Model DSA-031F-12 EU 12, Input 100-240V AC, Output 12V DC 1A, TUV Certified
Physical size	5.72 x 4.92 x 2.9 in (145 x 125 x 74 mm.)
Weight	0.53 lbs (0.24 kg)
Antenna	Internal software-configurable antenna array with six directional, high-gain elements (four vertical and two horizontal) and 63 unique antenna patterns
Ethernet ports	1 auto MDX, auto sensing 10/100 Mbps, RJ45 port
LED display	Antenna Power LAN Wireless Air Quality
Environmental conditions	Operating Temperature: $32^oF – 104^oF$ ($0^oC – 40^oC$)
	Operating Humidity: 15% - 95% non condensing
Electromagnetic Emissions	Meets requirements of FCC Part 15 Class B

Management

Configuration and monitoring interface	Ruckus Wireless Web User Interface (WebUI)

Login	Username: **admin** Password: **password**
Statistics	LAN, wireless and associated remote APs Accessible via Ruckus Wireless Web Interface
Software update	Via FTP, TFTP, or Web download Accessible via Ruckus Wireless Web Interface
Other Utilities	System Support Snapshot
Others	
Standards/Specifications	802.11 b/g 802.11u 802.11e, Wi-Fi Alliance WMM
Channels	US/Canada: 1-11 Europe (ETSI X30): 1-13 Japan X41: 1-13
RF Power output	23 dBm for 802.11b 23 dBm for 802.11g
Certifications	FCC, IC-03, CE, Telec, VCCI, C-Tick
Wireless Security	WEP, WPA-PSK, 802.1X